Antro Neuvonen

WLAN-tietoturvan testaus

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietoverkot

Insinöörityö

05.11.2013

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Antro Neuvonen WLAN-tietoturvan testaus 34 sivua 5.11.2013
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoverkot
Ohjaaja(t)	yliopettaja Janne Salonen

Työn tarkoituksena on käsitellä kevyesti WLAN-tietoturvaan liittyviä seikkoja. Tässä työssä käydään teoreettisesti läpi, kuinka kotona voi yrittää testata omaan WLAN:iin liittyvää tietoturvaa ja siihen kohdistuvia uhkia. Työ on perusohje kaikille, jotka ovat huolissaan langattoman verkkonsa yksityisyydestä.

Työ pohjautuu pääasiassa teoriaan ja jonkin verran testaukseen aircrack-ng-nimisen ohjelman avulla. Testit tehtiin käyttämällä kannettavaa tietokonetta sekä kotitietokonetta ja siihen kytkettyä WLAN-reititintä. Päätavoitteena oli kyetä murtamaan WLAN:in salasana ja tunkeutua langattomaan verkkooni käyttämällä apuna aircrack-ng-ohjelmaa.

Havainnot olivat pääasiassa sellaisia, että jos käyttää heikkoja salasanoja tai salausta, on melko helppoa murtaa ne, vaikka ei olisi erityisen harjaantunut hakkeri. Valitettavasti internet on pullollaan ohjelmia, joita voi käyttää laittomaan toimintaan.

Työn tulokset osoittavat, että langattomaan tietoverkkoon liittyy tietoturvauhkia ja kaikkien pitäisi käyttää ainoastaan vahvoja salasanoja: WPA- tai WPA2-salausta sekä piilottaa verkon SSID.

Avainsanat	WLAN, tietoturva, tietoturvatestaus

Author(s) Title Number of Pages Date	Antro Neuvonen Testing WLAN Security 34 pages 5 November 2013
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Janne Salonen, Principal Lecturer

The purpose of this study is to deal lightly with security issues regarding wireless networks. This work looks at the theory of how wireless network security and the threats against it can be tested at home. This study is provides a basic guideline to everyone who is concerned about their wireless network's privacy.

This study is mainly based on theory and some testing made principally with a program called aircrack-ng. The tests were made with a laptop and home pc. The main goal was to crack my own WLAN password and penetrate to my wireless network with the help of aircrack-ng.

The findings of this study indicate that if one uses weak passwords and weak encryption it is fairly easy to crack them and penetrate to the system even if you are not very experienced or familiar with hacking. Sadly the Internet is full of different kind of programs which can be used for illegal purposes.

Based on the results of this study, it can be concluded that there are security issues with wireless networks and everyone should use only strong passwords and WPA or WPA2 encryption and also hide their network’s SSID.

Keywords	WLAN, security, security testing

Sisällys

Lyhenteet

1 Johdanto 1

2 WLAN 2

2.1 Yleistä 2

2.2 Käyttökohteet 2

2.3 Yhteystekniikat 3
2.3.1 Infrapunatekniikka 3
2.3.2 Radiotekniikka 3

2.4 IEEE-standardit 4
2.4.1 802.11 4
2.4.2 802.11n 4
2.4.3 802.11ac 5

3 WLAN-laitteet ja niiden tietoturva 6

3.1 Langattomien verkkojen tietoturva 6

3.2 SSID 7

3.3 Pääsylistat eli suodatuslistat 8

3.4 Autentikointi 8

3.5 Salausprotokollat 9
3.5.1 WEP 10
3.5.2 WPA (TKIP) 10
3.5.3 WPA2 (AES) 11

4 Tietoturvauhat 11

4.1 Brute force attack 11

4.2 Rogue access points/Ad-hoc networks 12

4.3 Denial of service (DoS) 12

4.4 Määritysongelmat 13

4.5 Mies välissä -hyökkäys, Man-in-the-middle attack, MITM attack 14

4.6 Radiotien salakuuntelu 15

4.7 Tietoinen verkon häirintä 15

5 Tietoturvatestaus 15

5.1 Testauksen apuvälineitä 16
5.1.1 Testaustekniikat 16
5.1.2 Testitapausten ja testien hallinnointi 17
5.1.3 Tietoturvatestauksen työkalut 17

5.2 Wireshark 18

5.3 Verkkojen etsintä ja haistelu 19

5.4 WEP-avaimen murtaminen 20

5.5 WPA/WPA2-salauksen murtaminen 22

6 Yhteenveto 30

Lähteet 33

Lyhenteet

AES	Advanced encryption mode on lohkosalausmenetelmä.
ASCII	American Standard Code for Information Interchange on 7-bittinen eli 128 merkkipaikan laajuinen tietokoneiden merkistö, joka sisältää ensisijaisesti amerikanenglannissa tarvittavat kirjaimet, numerot, väli- ja erikoismerkkejä sekä eräitä ohjauskoodeja.
b	Bitti. Pienin informaation yksikkö. Bitillä on kaksi mahdollista arvoa, joita kuvaavat yleensä ykkönen ja nolla.
B	Tavu. Kahdeksan bitin muodostama informaation yksikkö.
BSS	Basic service set on yksi SSID:n variaatio.
CRC	A cyclic redundancy check on usein käytetty virheen havaitsemisen koodi, jolla esimerkiksi tietoverkot havaitsevat muutoksia lähetetyssä datassa.
EAP	Extensible authentication protocol on käyttäjien tunnistusprotokolla.
EAPOL	Extensible authentication protocol over lan on paketointitekniikka, jolla IEEE 802.1X protokollan EAP-viestit kuljetetaan.
ESS	Extended service set on yksi SSID:n variaatio.
ETSI	European Telecommunications Standards Institute. Riippumaton, voittoa tavoittelematon eurooppalainen telealan standardisoimisjärjestö.
HIPERLAN	High Performance Radio Local Area Networks. ETSI:n standardoima nopea langaton lähiverkko, jonka siirtonopeus on 20 Mbit/s tai jopa 54 Mbit/s.
IBDD	Independent Basic Service Set on yksi SSID:n variaatio.

IEEE	Institute of Electrical and Electronics Engineers. Kansainvälinen tekniikan alan järjestö.
kbps	Kilobittiä sekunnissa. Tiedonsiirtonopeuden mittayksikkö.
LMSC	LAN MAN Standards Committee. Kehittää ja ylläpitää verkkojen standardeja.
MAC	Media Access Control. IEEE 802 -verkoissa verkon varaamisen ja itse liikennöinnin hoitava osajärjestelmä.
Mbps	Tiedonsiirtonopeus, megabittiä sekunnissa = 1000 kb/s, 1 000 000 b/s.
QoS	Quality of Service. Termi, jolla tarkoitetaan verkon tietoliikenteen luokittelua ja priorisointia.
RC4	Laajimmin käytössä oleva jonosalauksen menetelmä.
SSID	Service set identifier on langattoman lähiverkon verkkotunnus.
WEP	Wired equivalent privacy on turva-algoritmi langattomille tietoverkoille.
Wi-Fi	Wireless Fidelity. Langattoman verkon vaihtoehtoinen nimitys.
WLAN	Wireless local area network. Langaton lähiverkkotekniikka.
WPA	Wi-Fi protected access on välivaiheen tietoturvatekniikka

1 Johdanto

Tietoturvaan liittyvät asiat ovat askarruttaneet mieliä luultavasti jo niin kauan, kuin on ollut tarvetta salata tietoa. Varhaisimmat kryptografiaan liittyvät tiedot ovat jo muinaisen Egyptin ajoilta, jolloin tietoa salattiin kirjoittamalla viesti kaljuksi ajeltuun päähän ja annettiin tämän jälkeen hiusten kasvaa, jolloin viesti oli salattu ja valmis lähetettäväksi. Luonnollisesti tämän kaltainen viesti on helppo murtaa ja saada esiin lukukelpoisena.

WLAN-laitteiden yleistyessä on myös tarve niiden tietoturvan parantamiselle kasvanut. Nykyisin langattomia verkkoja löytyy lähes joka paikasta, kahviloista, hotelleista, työpaikoilta ja kodeista. Näihin langattomiin verkkoihin kytkeydytään kannettavilla laitteilla yhä enemmän. Älypuhelinten, kannettavien tietokoneiden, tablettien ja muiden kannettavien laitteiden määrän lisääntyessä, myös langattomien verkkojen käyttö lisääntyy. Sen takia myös tarve parantaa niiden tietoturvaa kasvaa ja langattomia verkkoja uhkaavatkin nykyisin yhä useammat tietoturvauhat kuin koskaan aiemmin [1.].

Tässä työssä on tarkoituksena tarkastella langattomiin lähiverkkoihin liittyvää tietoturvaa ja mahdollisuuksia testata sitä luotettavasti. Tietoturvan testaamiseen on kehitetty maksullisia ja maksuttomia ohjelmia esimerkiksi Aircrack-ng, joka pitää sisällään useita hyödyllisiä ohjelmia ja ominaisuuksia langattoman verkon turvallisuuden testaamiseen liittyen. Ilmaisia ohjelmia on muitakin, niistä muutamia käsitellään tässä työssä yllämainitun lisäksi. Maksulliset ohjelmat tuottavat yleensä parempaa tietoa turvallisuudesta, mutta tässä työssä keskitytään maksuttomiin ohjelmiin siitä syystä, että useimmat kuluttajat suosivat maksuttomuutta. Aluksi käsitellää WLAN-tekniikkaa ja siihen liittyviä standardeja.

Standardeista käydään läpi vain tämän hetken tärkeimmät ja niistäkin tarkemmin ainoastaan uutta 802.11ac-standardia, koska työn tarkoituksena ei ole selostaa WLAN:iin liittyvää teknologiaa, vaan selvittää tietoturvaan ja siihen liittyvien uhkien testaamista ja tietoturvauhkien minimointia. Koska 802.11ac-standardi on täysin uusi, sitä käsitellään hieman tarkemmalla tasolla.

2 WLAN

2.1 Yleistä

WLAN on langaton lähiverkkotekniikka, jolla erilaiset verkkolaitteet voidaan liittää ilman kaapeleita. WLAN-termillä tarkoitetaan usein IEEE 802.11 -standardia, mutta myös ETSI:n standardoima HiperLAN on langaton lähiverkko. Yleisessä kielenkäytössä kuitenkin termeillä WLAN, 802.11 ja Wi-Fi tarkoitetaan samaa asiaa. WLAN:ia käytetään usein WLAN-tukiaseman ja –-reitittimen kautta.

Kuva 1. Kuvassa D-Linkin WLAN-tukiasema ja -reititin.

2.2 Käyttökohteet

WLAN:ia käytetään yleisesti kotona, työpaikoilla ja julkisissa tiloissa. Kodeissa vältetään kaapelointien tekemistä erilliseen sisäverkkoon, kun esimerkiksi kotiin tulevaan kaapelimodeemiin liitetään erillinen langaton tukiasema, ellei modeemissa jo ole sellaista oletuksena. Nykyisin esimerkiksi televisioissa on usein WLAN -ominaisuudet.

Sitä kautta kuluttaja pääsee näppärästi internetiin hyödyntämään interaktiivista sisältöä, vaikka vuokraamalla videon tai pelaamalla pelejä verkossa.

Monet yritykset tarjoavat maksutta tai maksua vastaan WLAN-yhteyden asiakkaiden käytettäväksi esimerkiksi älypuhelimella tai kannettavalla tietokoneella. Käytännössä kaikilla lentoasemilla on maksuton WLAN-yhteys käytettävissä matkustajille.

2.3 Yhteystekniikat

Yhteydet voidaan muodostaa lähiverkoissa joko radiotietä tai infrapunaa käyttäen.Radiotie on yleisimmin käytetty tekniikka sen huomattavasti paremman kantavuuden ja suuntaamistarpeen puuttumisen takia.

2.3.1 Infrapunatekniikka

Nimensä mukaisesti infrapunatekniikka siirtää tietoa valon muodossa laitteiden välillä. Lyhyen kantamansa takia tekniikka soveltuu lähinnä laitteille, jotka ovat lähellä toisiaan ja näköyhteydessä. Ympäriinsä säteileviäkin laitteita on kehitetty, mutta niissä heikkoutena on mahdolliset vastaanottimen ja lähettimen välissä olevat esteet, jotka aiheuttavat merkittävää vaimennusta.

2.3.2 Radiotekniikka

Radiotekniikoita, joita käytetään, ovat kapeakaistatekniikka sekä hajaspektritekniikka. Kapeakaistatekniikassa käytetään nimensä mukaisesti kapeita kaistoja ja eri käyttäjille määritellään omat kanavataajuudet, ettei pääse syntymään ylikuulumisia.

Hajaspektritekniikasta on käytössä kahdenlaista lähetysstandardia: suorasekvenssitekniikka ja taajuushyppelytekniikka. Hajaspektritekniikan hyvänä puolena on se, että tiukkojen lähetystehojen rajoitusten suhteen sen rinnalla voidaan käyttää muitakin langattomia lähiverkkoja ilman, että ne häiritsevät toisiaan.

2.4 IEEE-standardit

IEEE eli Institute of Electrical and Electronics Engineers on maailman suurin tekniikan alan järjestö, joka on omistautunut teknisten innovaatioiden kehittämiseen ja edistämiseen. Sen missiona on edistää teknologista innovointia ja huippuosaamista ihmiskunnan hyväksi. Järjestö ja sen jäsenet tuottavat erilaisia arvostettuja julkaisuja, konferensseja, teknologian standardejasekä ammatti- ja koulutusaktiviteetteja. [2.]

Voimassa olevia IEEE-standardeja on kaikkiaan yli 900. Langattomaan lähiverkkoon liittyviä ovat 802.11-standardit. Suosituimpina tällä hetkellä ovat 802.11b ja 802.11g. Ensimmäinen WLAN-standardi julkaistiin vuonna 1997. [3.]

802.11-standardin kehitys on jaettu eri työryhmille, joista jokainen keskittyy omaan standardiinsa. Työryhmät ovat osa IEEE LMSC:tä.

2.4.1 802.11

Ensimmäinen WLAN-standardi määrittää pääasiassa OSI-mallin fyysisen kerroksen ja siirtokerroksen alemman osan, joka tunnetaan nimellä MAC. [3] Standardin määrittelemät verkkoyhteyksien nopeudet ovat 1 Mbps ja 2 Mbps.

2.4.2 802.11n

Tällä hetkellä käytetyin standardi tunnetaan myös nimellä IEEE 802.11n-2009. Sen korvaajaksi on suunniteltu 802.11ac-standardia vuoden 2013 lopussa. Standardi käyttää hyväkseen useita antenneja lisätäkseen siirtonopeuksia. Aikaisempien versioiden, kuten 802.11a ja 802.11g, tiedonsiirtonopeuksista onkin tällä tekniikalla päästy 54 Mbit/s jopa teoreettiseen 600 Mbit/s nopeuteen käyttämällä neljää samanaikaista tilallista lähetysvirtaa (spatial stream) 40 Mhz:n kanavanleveydellä.

802.11n käyttää niin sanottua MIMO-tekniikkaa (Multiple-Input and Multiple-Output), jossa lähetyksen vastaanottoon ja lähettämiseen käytetään samanaikaisesti useampaa kuin yhtä antennia. Tätä usean samanaikaisen signaalin lähettämistä ja vastaanottamista kutsutaan nimellä tilallinen limittäminen (spatial multiplexing). Jokainen signaali lähetetään oman spektrikanavan kautta, jotta vältetään yhteentörmäykset.

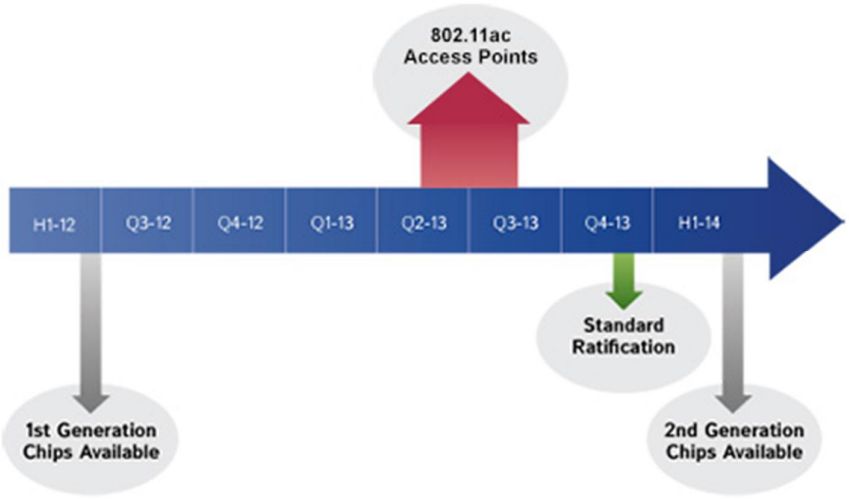
2.4.3 802.11ac

Tämän hetken tuorein WLAN-standardi 802.11ac ei ole vielä täysin valmis Tosin julkaisu on tapahtunut jo niin, että laitteiden valmistajat voivat sitä hyödyntää. Standardin ratifioinnin on tarkoitus tapahtua vuoden 2013 viimeisellä vuosineljänneksellä.

Standardin teoreettinen nopeus on jopa 1,3 Gbps ja sen kattavuus on parempi, kuin edeltäjänsä 802.11n:n, mutta nopeus on periaatteessa ainoastaan teoreettinen, sillä todellinen nopeus määräytyy sen mukaan, kuinka nopea yhteys on todellisuudessa internetyhteyden palveluntarjoajalta langattomaan tukiasemaan. Kaistanleveyden kattavuus on 5 Ghz, mutta todellisuudessa kaistanleveys on jopa pienempi kuin edeltäjien 802.11n ja 802.11g 2,4 Ghz. [4]

Tällä hetkellä standardia tukevia päätelaitteita ei ole juurikaan valmistettu, vaan niiden odotetaan yleistyvän vasta vuonna 2015 ja ylittävän miljardin myydyn laitteen rajan. Tällä hetkellä muutamat valmistajat tuottavat piirisarjoja, jotka tukevat 802.11ac -standardia, esimerkiksi Intel, Marvell ja Qualcomm.

Erot, joita uusi tekniikka tuo tullessaan verrattuna vanhempaan 802.11n-standardiin ovat merkittäviä. Uusi standardi tukee 256-QAM-modulointitekniikkaa, jossa hyödynnetään tehokkaampaa virheenkorjausta. Koska jokainen datasignaali noudattaa tiettyjä rakennesääntöjä, voidaan virhetilanteet havaita ja korjata automaattisesti.802.11ac hyödyntää 256-QAM-modulointitekniikalla 3/4 ja 5/6 virheenkorjausta, mikä tarkoittaa sitä, että tarpeeton bitti syötetään joka kolmannelle ja viidennelle bitille



Kuva 2. 802.11ac-standardin aikataulu.

Nykyisin hallitsevana standardina on 802.11n, jonka korvaajaksi on tarkoitus tulla 802.11ac.

3 WLAN-laitteet ja niiden tietoturva

WLAN-laitteita valmistavia yrityksiä on lukematon määrä. Tunnetuimmat lienevät D-Link, TeleWell, Zyxell ja Cisco. Hinnat vaihtelevat muutamistä kymmenistä euroista satoihin euroihin.

Nykyisin langaton ominaisuus sisältyy jo useimpiin reitittimiin eikä niitä tarvitse erikseen hankkia. Yleensä reitititimet tulevat internetyhteyksiä tarjoavilta operaattoreilta kaupan päälle ja niille on annettu valmiiksi asetukset kuntoon, samoin kuin SSID, salasana sekä salausprotokolla. Tietoja voi käydä muuttamassa laitteen asetuksista, jos vain tietää pääkäyttäjän salasanan ja ip-osoitteen laitteeseen.

3.1 Langattomien verkkojen tietoturva

Langattomien verkkojen tietoturva koostuu useista menetelmistä, joilla pyritään estämään asiattomien pääsy käsiksi omaan lähiverkkoon. Tyypillisimpiä langattoman tieto-

turvaan liittyviä protokollia ovat lienee WPA ja WEP, joista WEP on jo aikansa elänyt ja turvaton tapa hoitaa langattoman verkon tietoturvaa. Molemmat, sekä WPA että WEP, ovat kuitenkin edelleen käytössä.

3.2 SSID

SSID on langattoman lähiverkon verkkotunnus, jonka avulla erotetaan samalla alueella olevat WLAN-verkot toisistaan ja voidaan kytkeytyä haluttuun verkkoon.

SSID:stä käytetään kahta variaatiota:

- Langattomat Ad-hoc verkot, jotka koostuvat asiakaslaitteista ilman liityntäpistettä, käyttävät tunnisteena IBSS ID:tä.
- Tukiasemalliset verkot, joissa liityntäpiste BSS tai vaihtoehtoisesti ESS käyttävät tunnisteena BSS ID:tä tai ESS ID:tä.

SSID:t ovat merkkijonoja, joissa kirjainkoko merkitsee eri merkkiä. Ne koostuvat yleensä jonosta aakkosnumeerisia merkkejä, ja niiden maksimipituus on 32 merkkiä. [5.]

Melkein poikkeuksetta, kun hankkii laajakaistayhteyden paikalliselta monopoliasemassa olevalta verkko-operaattoriltasi (esimerkiksi Elisalta), ja reititin sisältää langattoman yhteyden, asiakas saa myös automaattisesti operaattorin määrittelemän SSID:n tähän langattomaan reitittimeen. Se kannattaa ehdottomasti käydä muuttamassa, jos mahdollista, johonkin muuhun. Yleensä tiedot pääsee muuttamaan sillä tietokoneella, johon langaton reititin on kytketty käyttämällä web-selainta. Web-selaimen osoitekenttään kirjoitetaan http://<langattoman reitittimen IP-osoite> ja pyydetyt käyttäjänimi ja salana, jonka jälkeen käyttäjä pääsee langattoman reitittimen kotisivulle muokkaamaan tietoja. Yleensä SSID kannattaa pitää piilotettuna, mikä vähentää sen riskiä joutumasta väärien henkilöiden käsiin. Onneksi pelkkä SSID:n vuotaminen ulkopuolisille ei tarkoita, että verkko olisi suojaton.

3.3 Pääsylistat eli suodatuslistat

Pääsylistoja käytetään yleensä silloin, kun halutaan hallita IP-liikennettä, kun verkon koko kasvaa tai halutaan suodattaa paketteja, jotka kulkevat reitittimen läpi.

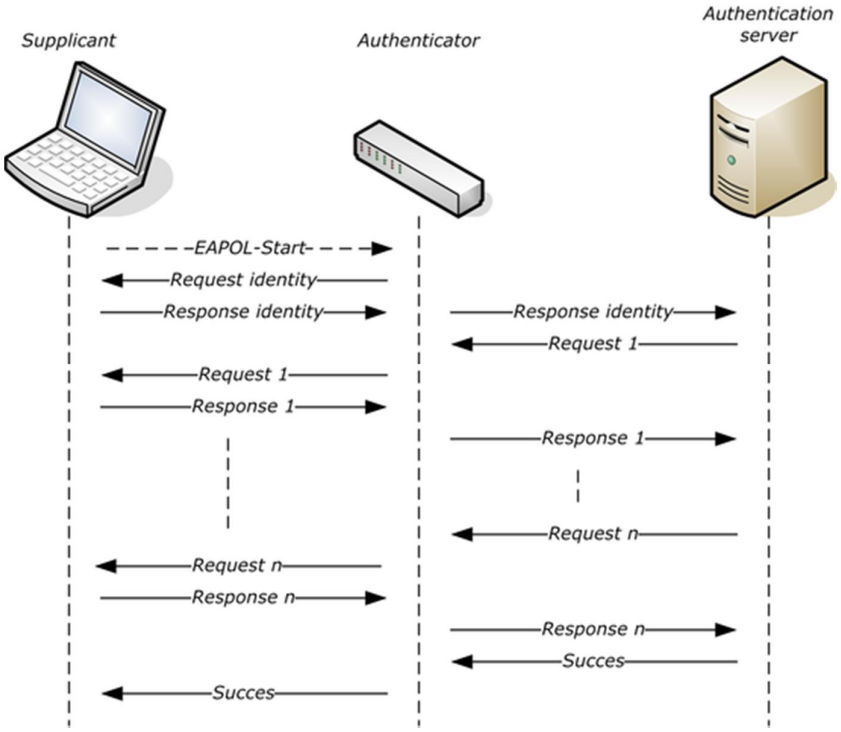
Pääsylistoilla voi kätevästi rajoittaa tai sallia liikennettä sen kulkiessa reitittimen läpi, reitittimen liitännän näkökulmasta liikenne on joko sisään tulevaa tai ulos lähtevää. Suodatuksella voidaan määritellä joustavasti, miten ja mitkä paketit pääsevät kulkemaan verkossa ja minkä verkkojen osien välillä. Näin voidaan määritellä, kuka pääsee käyttämään mitäkin verkon resurssia.

Pääsylistoja on useita, esimerkiksi standardipääsylistoja, jotka tarkastavat paketin lähdeosoitteen ja vertaavat sitä pääsylistan ehtoihin. Vertailun perusteella paketti joko hylätään tai lähetetään eteenpäin. Tämä vertailu perustuu lähteen verkon tai aliverkon tai isännän IP-osoitteeseen, joten se ei pysty erottelemaan yksittäisiä TCP/IP-protokollapinon protokollia. Toinen pääsylista on laajennettu pääsylista, jossa tarkastetaan paketista sekä lähde- että kohdeosoite. Laajennettu IP-pääsylista voi myös tarkastaa TCP/IP-protokollapinon protokollia, porttinumeroita ja muita parametreja tehdessään lähetys- tai hylkäyspäätöksiä.

3.4 Autentikointi

Wlan client ei autentikoi tukiasemaa, tukiasema autentikoi clientin, mutta ei käyttäjää. Autentikointiin voidaan käyttää myös WEP:iä tai WPA:ta.

Autentikointiprotokollista esimerkiksi EAP-protokolla tukee useita tunnistustapoja, eikä ole itse varsinaisesti autentikointimenetelmä. EAP tukee muun muassa kertakäyttösalasanoja, älykortteja sekä käyttäjänimiä.



Kuva 3. EAP-prosessi

3.5 Salausprotokollat

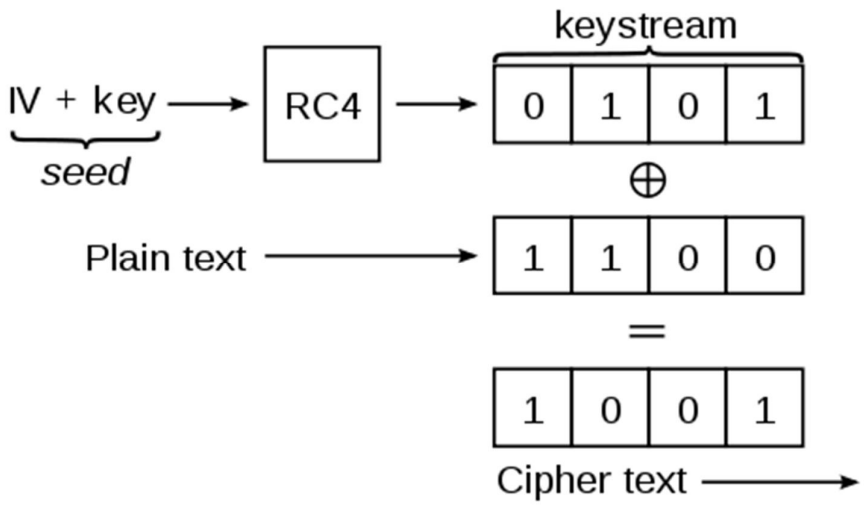
Salausprotokollalla tarkoitetaan tiedon salausta jollain salakirjoitusmenetelmällä. Paketti lähetetään salattuna, jajkun se saapuu vastaanottajalle, vastaanottaja purkaa koodatun tiedon vastaavalla avaimella. Salakirjoitusmenetelmiä on useita erilaisia, esimerkiksi Diffie-Hellman-avaimenvaihtoprotokolla tai RSA- ja ElGamal -kryptosysteemit.

Salausprotokollan tarkoituksena on turvata tietoliikennepakettien kulku siten, ettei kukaan ulkopuolinen taho pääse niitä muuttamaan tai kaappaamaan lähetyspisteen ja vastaanottajan välissä. Tietoliikennepakettien kulkuun liittyvät pakettivuon eheys; eli paketit tulevat oikeassa järjestyksessä, eikä pakettivuossa ole mitään ylimääräisiä tai poistettuja paketteja; pakettien todennus eli varmistetaan, että vastaanottaja ja lähettäjä todella ovat ne, joiden välillä juuri näiden pakettien kuuluukin liikkua; paketin eheys eli jokainen paketti tulee muuttumattoman perille ja lopuksi paketin luottamuksellisuus eli paketit eivät varmasti ole muiden kuin niille kuuluvien todennettujen osapuolien luettavissa ja käsiteltävissä.

3.5.1 WEP

WEP-salausmenetelmä oli osa vuonna 1999 julkaistua IEEE 802.11 -standardia. Sen tarkoituksena oli tehdä langattomasta lähiverkosta yhtä turvallinen käyttää kuin langallisestakin lähiverkosta [6]. Vaikka sen tarkoituksena onkin suojata tietoliikennettä langattomassa lähiverkossa, on sen salaus melko helppoa purkaa. Aluksi WEP-salausmenetelmä käytti ainoastaan 40-bittistä salausavainta, mutta myöhemmin kehitettyjen 802.11b ja 802.11g -standardien myötä käytössä on myös 64- tai 128-bittiset avaimet.

WEP käyttää jonosalausta, RC4:ää, luottamuksellisuuteen ja CRC-32:sta tiedon eheyden tarkistamiseen.



Kuva 4. WEP-suojausmenetelmä.

3.5.2 WPA (TKIP)

WPA tarjoaa vahvemman salauksen kuin WEP käyttämällä joko TKIP (temporal key integrity protocol) tai AES (advanced encryption standard) teknologiaa. WPA kehitettiin nimenomaan sen takia, että haluttiin paikata WEP:iin liittyviä heikkouksia [7]. TKIP tarjoaa parannuksen siten, että siinä on vaihtuva 128-bittinen avain, jonka se generoi dynaamisesti joka kerran, kun uusi paketti lähetetään.

WPA:n heikkous on, kun käyttäjät määrittelevät helposti murrettavia salasanoja. Tähän käytetään niin sanottua brute force attack -hyökkäystä.

3.5.3 WPA2 (AES)

WPA2 on korvannut WPA:n, ja se käyttää AES-perustaista lohkosalausta. AES on ainakin toistaiseksi ollut murtamaton, mutta luultavasti sekin tulee lähitulevaisuudessa murrettua. AES:ssa on kiinteä 128 bitin lohkokoko ja salakirjoitusalgoritmeissä käytettävät avainten koot voivat olla joko128, 192 tai 256 bittiä. Mitä suurempi avaimen koko, sitä enemmän EAP käyttää kierroksia tekstin salaukseen. Esimerkiksi 256 bitin avaimella tehdään salauskierroksia 14. Salaus puretaan tekemällä samat kierrokset käänteisessä järjestyksessä samalla salausavaimella, kuin ne oli salattukin.

4 Tietoturvauhat

4.1 Brute force attack

Heikkoja salasanoja on suhteellisen helppo murtaa käyttämällä brute force attack -metodia. Tämä hyökkäystapa on niin sanottu yritys ja erehdys -tyyppinen metodi, jossa automaattisella ohjelmalla yritetään murtaa salasanaa tai vaikka PIN-koodia syöttämällä satunnaisia merkkijonoja hyökkäyksen kohteena olevalle salasanasuojatulle sovellukselle tai tiedostolle, kunnes oikea salasana selviää ja hyökkääjä pääsee tietoihin käsiksi. Tyypillisimmät brute force attack -hyökkäykset ovat esimerkiksi niin sanottu sanakirjahyökkäys, jossa syötetään kaikki sanakirjasta löytyvät sanat ja yritetään niillä päästä suojauksen ohi. Toinen tapa käyttää hyökkäystä on syöttää tavanomaisimpia salasanoja tai kirjaimien ja numeroiden yhdistelmiä. Qwerty lienee käytetyin tyypillisimmistä salasanoista. Paras tapa suojatua tällaisia hyökkäyksiä vastaan on luoda kompleksinen erikoismerkkejä sisältävä salasana, joka on mahdollisimman pitkä, eikä käyttää esimerkiksi lemmikkien nimiä, kotiosoitetta tai vastaavia.

4.2 Rogue access points/Ad-hoc networks

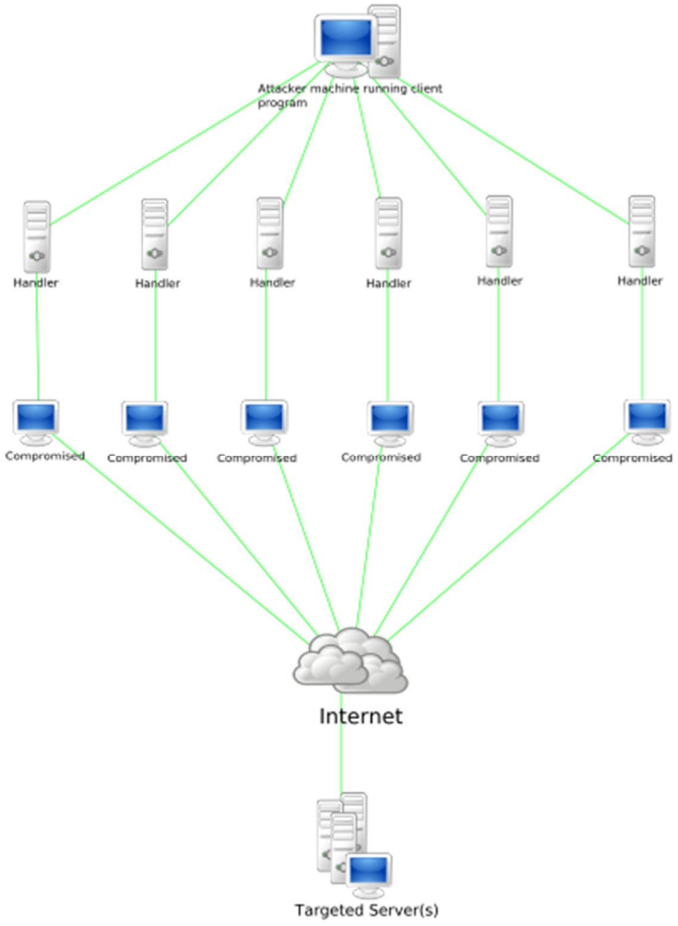
Rogue access point on mikä tahansa langaton tukiasema, joka on asennettu tietoliikenneverkon infrastruktuuriin ilman tietoliikenneverkon valvojan tai omistajan lupaa. [8.] Tällä tavalla ulkopuolinen pystyy tarjoamaan luvattoman pääsyn langattomalla yhteydellä langallisen verkon infrastruktuuriin.

Toinen, yleisempi tapa käyttää hyödyksi rogue AP:tä, on asentaa yrityksen ulkopuolelle langaton tukiasema, joka vastaanottaa yrityksen langattoman verkon lähettämää signaalia ja alkaa lähettää samanlaista signaalia, jolloin yrityksen työntekijät erehtyvät ottamaan yhteyden väärään niin sanottuun "evil twin" -signaaliin ja tällä tavalla mahdollistaen rikollisen pääsyn yrityksen tietoverkkoon.

4.3 Denial of service (DoS)

Palvelunestohyökkäys tarkoittaa verkkopalvelun lamauttamista niin, ettei verkkopalvelu ole enää täysin tai ollenkaan käytettävissä. Tämän tyyppisen hyökkäyksen tarkoituksena ei ole varsinaiseen järjestelmään tunkeutuminen, vaan ainoastaan toiminnan häiritseminen. Esimerkiksi pankkien verkkosivuille saatetaan tehdä DoS-hyökkäys, jolla estetään pankin palveluita käyttävien asiakkaiden pääsy pankin verkkosivustolle.

Kuvassa 2 esimerkki laajasta palvelunestohyökkäyksestä, jossa useista lähteistä samaan aikaan hyökätään kohdepalvelimelle. Tällaisesta hyökkäyksestä käytetään myös nimeä hajautettu palvelunestohyökkäys eli Distributed Denial of Service, DDoS. [9.]



Kuva 5. Kartta laajasta palvelunestohyökkäyksestä.

Tyypillisesti on olemassa kaksi eri DDoS-hyökkäystä, verkkokeskeinen hyökkäys, jossa verkkoa kuormitetaan niin, että kaistanleveys loppuu kesken ja verkko lakkaa toimimasta, ja sovelluskerroksen hyökkäys, jossa sovellusta kuormitetaan niin, että se ei enää vastaa yhteys- tai kyselypyyntöihin.

4.4 Määritysongelmat

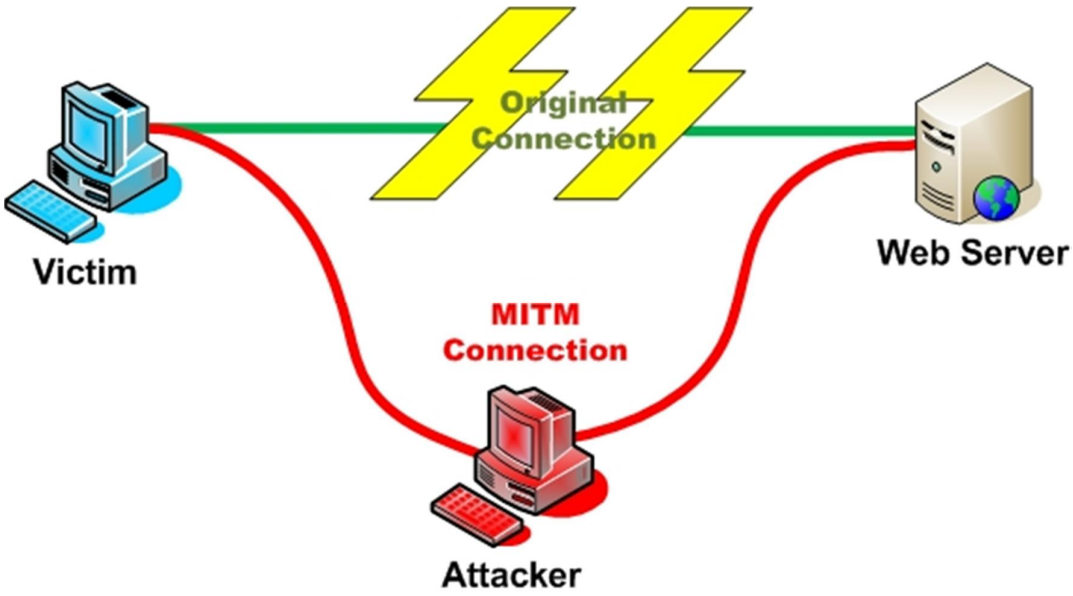
Väärin määritellyt tietoturva-asetukset tai muut laitteen asetukset ovat myös oma uhkansa. Jos laitteessa on määritelty asetukset väärin, ei mahdollisia tietoturva-asetuksia välttämättä voida korjata, ja järjestelmä on haavoittuvainen.

Määritysongelmiin voidaan vaikuttaa riittävällä ohjeistuksella, varsinkin liittyen salasanoihin. Yleensä ainakin yrityksissä on tarkat minimivaatimukset salasanojen kopleksisuudelle. Samoja sääntöjä voisi mainiosti käyttää myös kotikoneella.

4.5 Mies välissä -hyökkäys, Man-in-the-middle attack, MITM attack

Kyseessä on tietoturvahyökkäys, jossa hyökkääjä asettuu kahden osapuolen välisen tietoliikenteen välittäjäksi ja muuttaa halutessaan viestin sisältöä. Hyökkäyksessä hyökkääjä sieppaa viestin, jossa tapahtuu julkisen avaimen vaihto ja vaihtaa oman julkisen avaimen pyydetyn tilalle. Näin viestin alkuperäiset osapuolet luulevat, että he kommunikoivat yhä keskenään [10].

Hyökkääjä käyttää haittaohjelmaa, joka näyttäisi olevan viestin toisen osapuolen näkökulmasta serveri ja päinvastoin. Hyökkäyksen tarkoituksena on joko päästä lukemaan viesti tai päästä muokkaamaan viestiä, ennen kuin se saavuttaa määränpäänsä. Mies välissä -hyökkäys on tehokas http-protokollan ja tiedon lähettämisen luonteen takia, jotka ovat ASCII-muotoisia.



Kuva 6. Man-in-the-middle-hyökkäys.

Mies välissä -hyökkäys voidaan tehdä myös https-yhteyden yli käyttämällä samaa tekniikkaa kuin http-yhteydessäkin. Ainoana erona on, että yhteys koostuu kahdesta itsenäisestä SSL-istunnosta, yksi kummassakin TCP-yhteydessä. Selain muodostaa yhteyden hyökkääjän SSL-yhteyteen ja hyökkääjä muodostaa SSL-yhteyden web-palvelimelle. Yleensä selain antaa varoituksen, ettei digitaalinen sertifikaatti ole pätevä, mutta usein käyttäjät sivuuttavat varoitukset, koska he eivät ymmärrä uhkaa.

4.6 Radiotien salakuuntelu

Radiotien salakuuntelulla pyritään kaappaamaan liikennettä ja selvittämään WEP-salausavain, sallittuja MAC-osoitteita tai hyötydatan sisältöä. Jos murtautuja saa selville WEP-salausavaimen ja MAC-osoitteen, on hänellä esteetön pääsy tietoverkon sisälle. Sallittujen MAC-osoitteiden takia pääsyä on melkein mahdotonta estää, ja tunkeutumista on vaikea havaita.

4.7 Tietoinen verkon häirintä

Tietoista verkon häirintääkin voidaan pitää eräänlaisena tietoturvauhkana, vaikkei tietoturva varsinaisesti olekaan vaarassa, vaan häirinnällä pyritään lähinnä estämään liikennettä ja laskemaan verkon käytettävyyttä. Varsinaisen liikenteen muuttaminen on vaikea toteuttaa, joskaan ei täysin mahdotonta. Liikennettä voi muuttaa esimerkiksi aircrack-ng-nimisellä ohjelmalla, joka sisältää suuren määrän erilaisia työkaluja oman verkon testaukseen liittyen.

5 Tietoturvatestaus

Tietoturvatestauksen päätarkoituksena on turvata ohjelmistojen ja laitteiden turvallinen käyttö siten, ettei ulkopuolinen taho pääse väärinkäyttämään niitä, eikä pääse edes tarkastelemaan tiedostoja tai laitteen asetuksia. Tietoturva pitää sisällään luottamuksellisuuden, tietojen eheyden, tietojen vastuullisen käytön, kiistämättömyyden, autenttisuuden ja saavutettavuuden [11.]. Jos joku edellä mainituista on turmeltunut, tietoturvaa on rikottu ja syyt siihen on tutkittava mahdollisimman pian, sekä tukkia tietoturva-aukko heti, kun se on mahdollista.

Tietoturvatestauksen tärkeys kasvaa jatkuvasti, useat yritykset panostavatkin nykyistä enemmän tietoturvatestaukseen ja ottavat sen osaksi muita testausstrategioitaan. Tietoturvatestaus voidaan suorittaa erillisenä testauksena, mutta yleensä se kannattaa yhdistää muuhun testaukseen mukaan systeemitestaus, ja viimeistään hyväksymistestausvaiheessa. Testitapauksia suunniteltaessa ja kokonaistestaussuunnitelmaa tehdessä onkin hyvä muistaa, että tietoturvatestaus on tärkeä osa testausprosesseja.

5.1 Testauksen apuvälineitä

Testauksessa voidaan käyttää apuvälineinä esimerkiksi erilaisia maksuttomia tai maksullisia sovelluksia, jotka yrittävät murtaa langattoman verkon tietoturvan suojauksia. Testauksen kannalta on tärkeää, että käyttää useita eri ohjelmia, eikä vain yhtä, koska yksittäiset sovellukset eivät yleensä ole kovin kattavia, vaan keskittyvät lähinnä yhteen tai kahteen tapaan murtautua langattomaan verkkoon.

Paras tapa testata kotona langattoman verkon tietoturva-aukkoja ja turvallisuutta on yrittää murtautua omaan langattomaan verkkoon ja löytää mahdolliset ongelmat, kuten heikot salasanat, tietoturvaan liittyvät aukot ja paljastaa mahdolliset "rogue access point" -tyyppiset hyökkäykset. Kuluttajille on saatavilla useita ilmaisia ohjelmia, joita voi käyttää testauksessa ja niitä käydään läpi myöhemmin.

Yleensä kannattaa tutustua tietoturvatestauksesta kertovaan kirjallisuuteen tai internetistä löytyvään materiaaliin ja seurata alan julkaisuja, koska sieltä löytyy viimeisin tieto havaituista tietoturvapuutteista ja keinoista suojautua hyökkääjiä vastaan.

5.1.1 Testaustekniikat

Mielestäni testaustekniikka on yksi testauksessa käytettävistä apuvälineistä, vaikkei se varsinaisesti olekaan mikään väline, vaan ainoastaan tapa suorittaa testejä. Jokaisella testaajalla on oma sovellettu tekniikkansa, vaikka tekniikoista onkin kirjoitettu varsin laajalti ja niitä myös noudatetaan, toisia tarkemmin, toisia enemmän soveltaen.

Miten testitapaukset syntyvät? Miltä testitapaus näyttää? Näihin kysymyksiin yritän löytää joitain vastauksia tässä ja seuraavissa luvuissa. Testaaminen yhdistää tekniikoi-

ta, jotka keskittyvät testaajiin, kattavuuteen, mahdollisiin ongelmiin, toimintaan ja arviointiin. [12.]

5.1.2 Testitapausten ja testien hallinnointi

Testatessa mitä tahansa ohjelmistoja, sulautettuja tietojärjestelmiä, verkkoyhteyksiä tai vaikka tietoturvaan liittyviä asioita, kannattaa testauksessa käyttää apuvälineitä, varsinkin testitapausten hallinnoinnissa. Ehkä parhaiten tunnettu ja laajimmin käytetty testauksen apuväline on HP Quality Center, jonka viimeisin vakaa julkaistu versio on 11.5. Ohjelma on Hewlett-Packardin kehittämä, se on erittäin monipuolinen työkalu testauksessa. HP Quality Center, jonka ohjelmistojen laadunvarmistukseen on integroitu, vaatimusmäärittelyiden ylläpito, testien ylläpito ja liiketoiminnan prosessien testaus. Tähän ohjelmistoon saa myös yhdistettyä HP Quick Test Pro -ohjelmiston, jolla voidaan automatisoida usein toistettavia testejä, joiden manuaalinen ajaminen ei ole järkevää tai kustannustehokasta. Tällaisia testejä ovat yleensä regressiotestit, kun halutaan testata niitä toiminnallisuuksia, joihin ei ole varsinaisesti tehty muutoksia.

Muitakin ohjelmistoja on olemassa, joilla koko testauksen elinkaarta voidaan hallinnoida, esimerkiksi Bugzilla, joka on ilmainen, toisin kuin HP Quality Center. Henkilökohtaisesti voin kyllä todeta useita vastaavia ohjelmistoja kokeilleena, että HP Quality Center on niistä monipuolisin ja paras vaihtoehto käytettävyytensä ja hyödyllisten ominaisuuksiensa ja laajentamismahdollisuuksien takia.

5.1.3 Tietoturvatestauksen työkalut

Markkinoilla on useita tietoturvatestaukseen liittyviä ilmaisia ja maksullisia työkaluja, mutta melko vähän langattoman tietoverkon testaukseen liittyviä, mikä johtuu luultavasti siitä, ettei langattomaan verkkoon liittyviä tietoturvariskejä ole täysin tiedostettu. Ohjelmien kehittäjät sekä kuluttajat luottavat enemmän siihen, että omat palomuurit ja virustorjuntaohjelmat estävät väärinkäytökset, vaikka joku pääsisi käsiksi langattomaan tietoverkkoon. Onneksi nykyisin on jo joitain ohjelmia, joilla voidaan testata langattoman verkon haavoittuvuuksia.

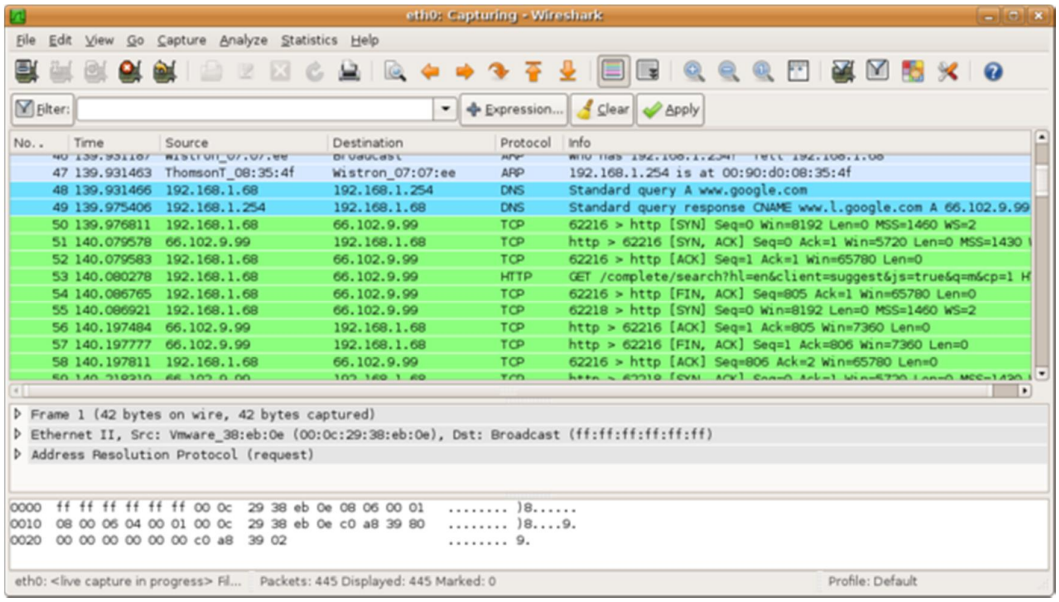
Seuraavissa luvuissa käydään läpi joitain ohjelmia, joilla voidaan testata oman langattoman verkon turvallisuutta. Huomioitavaa onkin, että kyseisiä ohjelmia tulee käyttää

ainoastaan oman verkon testaamiseen, ei ulkopuolisten verkkojen testaamiseen ilman asianomaisen verkon omistajan lupaa, koska se on laitonta ja voi johtaa vakaviin seuraamuksiin.

5.2 Wireshark

Wireshark on kätevä ohjelma, jolla voi analysoida tarkasti satoja eri protokollia liittyen tietoliikenteeseen. Ohjelman voi asentaa moniin eri käyttöjärjestelmiin, kuten Windowsiin ja Linuxiin. [13.]

Ohjelma on ilmainen ja sitä voi käyttää esimerkiksi verkossa olevien ongelmien ratkaisuun, analysointiin tai ohjelmien kehittämiseen. Metropoliassa sitä käytettiin muun muassa opetuksen tukena, joten kyseessä on monikäyttöinen ja laajalle levinnyt ohjelma. Käyttömukavuutta lisää se, että siinä on graafinen käyttöliittymä sekä joitain valmiiksi integroituja jaottelu- ja filtteröintiominaisuuksia.



Kuva 7. Wireshark GUI eli graafinen käyttöliittymä

Wiresharkia voi käyttää myös apuna, kun testataan langattoman tietoverkon tietoturvaa analysoimalla lähetettyjä ja vastaanotettuja paketteja sekä tarkastelemalla niiden sisältämää tietoa.

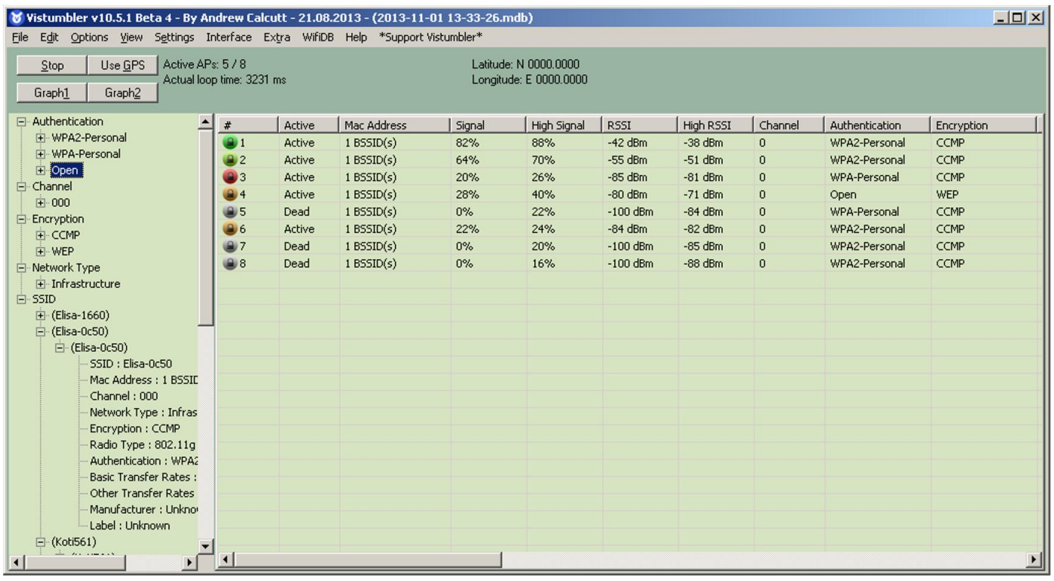
5.3 Verkkojen etsintä ja haistelu

Vaikka käytössä olisi kalliita langattoman tietoverkon spektrianalysaattoreita, kannattaa rinnalle ottaa kuitenkin myös maksuttomia vaihtoehtoja, koska ne voivat olla joissain tapauksissa käteviä ja nopeampia käyttää testaustilanteessa, kun esimerkiksi asennetaan uutta langatonta verkkoa tai ylläpidetään vanhaa.

NetStubler on tunnetuin ja yksi vanhimmista langattomia verkkoja havaitsevista testisovelluksista. Ohjelma näyttää lähistöllä olevat yhteyspisteet ja näyttää niiden perustiedot: SSID:n, kanavan, nopeuden, MAC-osoitteen, toimittajan ja salauksen. Ohjelma näyttää lisäksi, epätyypillisesti vastaaviin ohjelmiin, signaalin vahvuuden, kohinan ja signaali-kohinasuhteen. Tätä ohjelmaa on viimeksi päivitetty vuonna 2004, eikä se luultavasti toimi kunnolla uudemmilla käyttöjärjestelmillä, kuten Windows 7:llä. Ohjelma ei esimerkiksi näytä todellisia salausprotokollia, vaan riippumatta siitä, käyttääkö yhteyspiste WEP:iä, WPA:ta tai WPA2:ta, ohjelma näyttää salausprotokollan olevan WEP. Ohjelmaa voikin käyttää oikeastaan signaalin etsintään ja sen perustietojen tarkkailuun, sekä niin sanottuun wardrivingiin eli loiskäyttöön, jossa etsitään avoimia langattomia tietoverkkoja ajoneuvolla ympäriinsä liikkuen.

Kismet on avoimen lähdekoodin ohjelma, joka havaitsee langattomat lähiverkot ja kertoo niiden tietoja, kuten esimerkiksi SSID:n, vaikka se olisi piilotettu näkyviltä. Kismetiä päivitetään säännöllisesti ja viimeksi siitä on julkaistu uusi versio syyskuussa 2013. Ohjelmalla saa myös kaapattua langattoman verkon lähettimen ja päätelaitteen välillä kulkevia paketteja ja siirtää niitä esimerkiksi Wireshark:iin, TCPDump:iin tai muihin työkaluihin, joilla paketteja voi tarkastella ja käsitellä. Hyvä puoli tässä ohjelmassa on se, että se havaitsee myös tunkeutumisyritykset ja näin voi ohjelmaa hyödyntämällä testata esimerkiksi oman verkon haavoittuvuutta.

Vistumbler on avoimen lähdekoodin ohjelma, jolla voi skannata lähistöltä löytyviä langattomia verkkoja ja niiden yhteyspisteitä. Ohjelma näyttää laajasti tietoja ja on myös helposti muokattavissa omien tarpeiden mukaan.



Kuva 8. Vistumblerin pääsivu

Ohjelma näyttää SSID-tiedon, käytetyn salauksen ja myös sen, onko verkko ylhäällä vai ei. Ohjelmalla saa myös tuotettua erilaista grafiikkaa ja se näyttää signaalivoimakkuudet ja niin edelleen. Erikoista ohjelmassa on se, että sillä voi käyttää GPS:ää apuna ja seurata tosiajassa Google Earthia käyttämällä sijaintitietoja. Vistumbler näyttää myös mahdolliset rogue access pointit.[14.]

Verkkojen etsintään ja haisteluun käytettävillä ohjelmilla ei kuitenkaan varsinaisesti pysty murtautumaan langattomaan verkkoon, vaan niillä näkee ainoastaan enemmän ja vähemmän hyödyllisiä tietoja omasta verkosta ja myös mahdollisia rogue access pointeja, joilla pyritään väärinkäyttämään muiden verkkoja. Tietoja voi kuitenkin käyttää murtautumiseen, kuten myöhemmin näemme. Samoja tietoja nimittäin käytetään esimerkiksi aircrack-ng:ssä, kun sillä murretaan WEP- tai WPA/WPA2-salauksia.

5.4 WEP-avaimen murtaminen

Periaatteessa WEP-avaimen murtaminen on erittäin helppoa sen tunnettujen heikkouksien takia, esimerkiksi heikkojen avaimien luominen, jota on yritetty parantaa. Aircrack-ng:llä voi yrittää murtaa WEP-avaimen seuraavalla tavalla, mutta muitakin tapoja tietysti löytyy.

Ensin kortti täytyy asettaa monitorointitilaan käyttämällä komentoa airmon-ng start wlan0 9, missä:

- start wlan0 käynnistää wlan0 rajapinnan
- 9 on kanava, jolla kortti toimii.

Tämän jälkeen testataan, onko testattava kortti yhteyspisteen kantomatkan päässä ja voiko siihen injektoita paketteja komennolla aireplay-ng -9 -e karhu -a 00:33:32:31:5E ath0, missä:

- -9 tarkoittaa injektointitestiä
- -e karhu on langattoman verkon nimi
- -a 00:33:32:31:5E on yhteyspisteen MAC-osoite
- ath0 on langattoman liitännän nimi.

Injektiotestin jälkeen käynnistetään airodump-ng, jolla kaapataan muodostetut IV:t eli initializing vectorit eli yksinkertaisuudessaan mielivaltaiset numerot, joita käytetään salausavaimen kanssa tiedon salaamiseen. Tätä varten täytyy avata toinen konsoli käyttöön ja kirjoittaa sinne komento airodump-ng -c 9 --bssid 00:33:32:31:5E -w tiedosto ath0, missä:

- -c 9 on langattoman verkon kanava
- --bssid 00:33:32:31:5E on yhteyspisteen MAC-osoite
- -w tiedosto on se tiedosto, minne kaapatut IV:t kirjoitetaan talteen.

Jotta yhteyspiste ottaisi vastaan paketteja, täytyy lähteen MAC-osoite olla yhdistetty, koska muussa tapauksessa yhteyspiste hylkää paketin ja lähettää niin sanotun de-authentication paketin suojaamattomana eikä siinä tapauksessa uusia IV:tä muodosteta. Jotta MAC-osoite saadaan assosioitua yhteyspisteeseen, täytyy käyttää valheellista autentikointia komennolla aireplay-ng -1 0 -e karhu -a 00:33:32:31:5E -h 00:33:3C:3F:5A ath0, missä:

- -1 tarkoittaa valheellisen autentikoinnin tekemistä
- 0 on uudelleenliittymisen ajoitus sekunneissa

- -e karhu on langattoman verkon nimi
- -a 00:33:32:31:5E on yhteyspisteen MAC-osoite
- -h 00:33:3C:3F:5A on oman kortin MAC-osoite, jolta yhteys tehdään
- ath0 on langattoman interfacen nimi.

Kun yhteys on luotu, voidaan aireplay-ng käynnistää ARP-pyyntöjen uusinnan tilassa komennolla aireplay-ng -3 -b 00:33:32:31:5E -h 00:33:3C:3F:5A ath0. Komento aloittaa ARP pyyntöjen kuuntelun ja heti, kun se sellaisen kuulee, se alkaa välittömästi injektoida paketteja.

Seuraavaksi tarvitseekin enää ajaa aircrack-ng, että WEP-avain saadaan haltuun ja sen voi tehdä uudessa konsolissa komennolla aircrack-ng -b 00:33:32:31:5E tiedosto*.cap, missä:

- -b 00:33:32:31:5E spesifioi tietyn yhteyspisteen, jonka WEP avain halutaan löytää
- tiedosto*.cap valitsee kaikki tiedosto-alkuiset tiedostot ja jotka päättyvät .cap. Tässä tiedostossa oli siis tallessa aiemmin saadut IV:t.

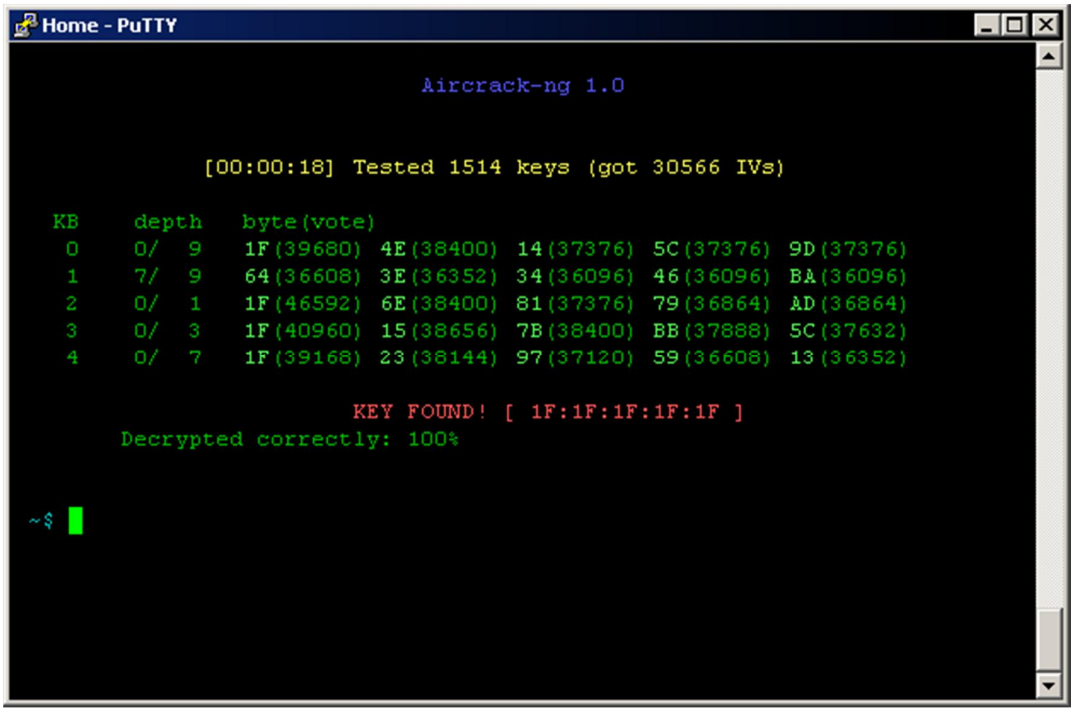
Jonkin ajan kuluttua ohjelma on saanut laskettua WEP-avaimen ja näyttää sen ruudulla. Teoriassa tarvitaan noin 250 000 IV:tä, jos halutaan murtaa 64-bittinen salaus ja 1 500 000 IV:tä, jos halutaan murtaa 128-bittinen avain.

5.5 WPA/WPA2-salauksen murtaminen

Saatavilla on useita erilaisia työkaluja, joilla voidaan murtaa langattoman tietoverkon kryptaus, joko käyttämällä hyväksi tunnettuja WEP:iin liittyviä heikkouksia tai käyttämällä brute force -hyökkäystä WPA:ta tai WPA2:ta vastaan. WEP-salausta ei oikeastaan kannattaisi edes käyttää suojaamaan langatonta tukiasemaa, koska se on auttamattomasti vanhentunutta tekniikkaa ja helppo murtaa. WPA/WPA2 ovat turvallisempia, varsinkin, jos käyttää pitkiä, yli 13-merkkisiä salasanoja, joissa on sekaisin isoja ja pieniä kirjaimia sekä erikoismerkkejä. Tällöin niiden murtaminen käyttämällä brute force -tekniikkaa on jotakuinkin mahdotonta. Pääperiaatteena voisi todeta, että mitä komplek-sisempi salasana, sitä vaikeampi sitä on murtaa. Seuraavissa luvuissa käydään läpi

joitain ohjelmia, joilla voi testata oman salasanansa vahvuutta ja jotka auttavat ymmärtämään langattoman tietoverkon salasanojen heikkouksia.

Aircrack-ng on avoimen lähdekoodin kokoelma erilaisia ohjelmia, joita voi käyttää WEP- ja WPA/WPA2-salausavainten murtamisessa ja sillä voi kaapata datapaketteja, injektoida ja toistaa liikennettä. Injektoinnilla tarkoitetaan sitä, että yritetään vaikuttaa käynnissä olevaan liikenteeseen rakentamalla uusia paketteja niin, että ne vaikuttavat kuuluvan normaaliin liikenteeseen. Pakettien injektointia käytetään yleisesti man-in-the-middle-hyökkäyksessä [15] tai denial of service -hyökkäyksessä.



Kuva 9. Aircrack-ng pääsivu

Ohjelman käyttäminen alkaa sillä, että ensin se asennetaan koneelle, jonka jälkeen määritellään asetukset. Ensimmäisenä etsitään oman langattoman kortin piirisarjan valmistajan tieto, koska aircrack-ng ei tue kaikkia piirisarjoja. Varsinkin Windows-käyttöjärjestelmillä on rajoitteita ja ongelmia aircrack-ng:n käytön kanssa. Kaikkein helpoimmalla ohjelman kanssa pääsee sillä, että käyttää Linuxia. Tärkeitä asioita, joita tulee ottaa huomioon ohjelmaa asentaessa ovat käyttöjärjestelmä, mitä kautta piirisarja on kytketty koneeseen ja mitä ominaisuuksia ohjelmasta haluaa käyttää.

WLAN-kortti on oikeastaan kahden eri valmistajan tekemä, varsinaisen kortin valmistaja, esimerkiksi D-Link tai Linksys ja kortin piirisarjan valmistaja ja se on juuri se tieto, mitä tarvitaan, jotta aircrack-ng:tä voidaan käyttää. Se on myös yleensä hankalin selvitettävä. Piirisarjan nimen voi selvittää esimerkiksi etsimällä internetistä hakusanoilla ”<kortin malli> piirisarja” ja yleensä sillä tavalla voi löytää tietoa oman korttinsa piirisarjasta. Piirisarjan nimeä voi myös yrittää etsiä Windowsin ajureiden nimistä, sillä yleensä ajureiden nimet vastaavat piirisarjoja. Ohjelma on valitettavasti tarkka siitä, että piirisarjan versionumeronkin täytyy olla oikein eli pelkästään kortin nimi ei riitä, vaan kortin versiokin täytyy tietää.

Linuxilla kortin ja piirisarjan selvittäminen voi olla todella helppoa ja nopeaa, esimerkiksi kirjoittamalla komentoriville käsky dmesg. Yleensä se kertoo, mikä kortti ja piirisarja on asennettu koneeseen. Jos kuitenkin käyttää Windowsia pääasiallisesti käyttöjärjestelmänä, niin voi harkita Linux distron käyttämistä, jolloin saa tavallaan molempien käyttöjärjestelmien parhaat puolet käyttöönsä.

Kun ohjelma on asennettu ja WLAN-kortin piirisarjan tieto saatu kaivettua esiin, alkaa varsinainen testaaminen. Aluksi täytyy varmistaa, että oma WLAN-kortti kykenee injektoimaan ja havaitsemaan ping-vasteaikoja yhteyspisteelle. Perusinjektiotesti antaa kallisarvoista tietoa. Ensinnäkin se listaa yhteyspisteet lähistöllä jotka vastaavat lähetystiedusteluihin ja toiseksi se tekee 30 paketin testin, joka kertoo yhteyden laadun. Lähetysten vastaanottoprosentti kertoo, kuinka hyvä yhteyden laatu on. Testiin voi myös sisällyttää yhteyspisteen nimen ja MAC-osoitteen, jolloin voidaan testata jotain tiettyä yhteyspistettä tai piilotettua SSID:tä.

Testaaminen tapahtuu lähettämällä tiedusteluja, jotka kysyvät miltä tahansa kantaman päässä olevalta yhteyspisteeltä tietoja itsestään. Läheskään kaikki yhteyspisteet eivät vastaa tämän tyyppisiin tiedusteluihin ja ne, jotka vastaavat, kootaan listaan myöhempää käyttöä varten. Jos yhteyspiste vastaa, siitä annetaan näytölle viesti, että kortti kykenee injektoimaan liikennettä. Ohjelma lisää jatkuvasti listalle yhteyspisteet, jotka tunnistetaan tiedustelupakettien kautta myöhempää prosessointia varten. Jos testin alkuvaiheessa oli spesifioitu tietty yhteyspiste antamalla sen SSID, niin sekin lisätään listalle.

Jokaiselle listalla olevalle yhteyspisteelle lähetetään tämän jälkeen esimerkiksi 30 suunnattua tiedustelupyyntöä ja jokaiselta yhteyspisteeltä saadut vastaukset ja niiden prosentuaalinen määrä näytetään näytöllä, jolloin saadaan tietää, voiko oma wlan-kortti kommunikoida yhteyspisteiden kanssa ja kuinka hyvin kommunikointi toimii.

Ennen varsinaista testaamista WLAN-kortista täytyy asettaa päälle valvontatila ja kanava käyttämällä komentoa airmon-ng <start|stop> <interface> [channel] tai airmon-ng <check|check kill>, missä:

- <start|stop> kertoo haluaako käyttäjä laittaa valvonnan päälle tai pois
- <interface> kertoo rajapinnan, esimerkiksi wlan0
- [channel] asettaa kortin tietylle kanavalle
- <check|check kill> check kertoo, jos joku käynnissä oleva prosessi häiritsee aircrack-ng ohjelman käyttöä ja check kill tarkastaa ja tappaa kyseiset prosessit.

Tämän jälkeen voidaan aloittaa testaaminen komennolla aireplay-ng -9 -e karhu -a 00:di:ce:fa:00 -i wlan1 wlan0, missä:

- -9 tarkoittaa injektiotestiä
- -e karhu tarkoittaa verkon nimeä (SSID), joka on valinnainen tieto
- -a 00:di:ce:fa:00 on yhteyspisteen MAC-osoite, joka on valinnainen tieto
- -i wlan1.

WPA/WPA2-algoritmin murtaminen kannattaa aloittaa niin, että ensin käy vaihtamassa PSK salasana johonkin yksinkertaiseen ja nopeasti murrettavaan reitittimen tietoturva-asetuksista, esimerkiksi anonymous. Murtamisen apuvälineenä voi käyttää BackTrack 5 -ohjelmaa, joka sisältää muun muassa aircrack-ng:n ja muita testauksessa hyödyllisiä sovelluksia. Testatessa tarvitaan luonnollisesti esimerkiksi kannettavaa tietokonetta, johon voi asentaa kaikki tarvittavat ohjelmat ja jossa on Wi-Fi-yhteys käytettävissä. Vastinparina tarvitaan langaton reititin ja mieluiten niin, että se on testaajan oma reititin, ettei aleta murtautumaan esimerkiksi naapurin reitittimeen, ellei siihen ole lupaa.

Itse testaaminen tehdään koneella, johon on asennettu BackTrack 5 -ohjelma. Aluksi asetetaan valvontatila päälle käyttämällä airmon-ng-komentoa muodossa airmon-ng start wlan0, jolloin monitorointi käynnistyy wlan0 interfacelle. Sen jälkeen tarkastetaan komennolla airodump-ng mon0, onko listalle ilmestynyt uusia interfaceja. Listalta pitäisi löytyä nyt sen interfacen tiedot, jonka tietoturvallisuutta yritetään testata. Listalta selviää myös laitteen SSID, sekä se, että kyrptauksessa käytetään WPA:ta. Näkyvissä on myös laitteen BSSID eli MAC-osoite. Monitorointi on tärkeää laittaa kortista päälle, koska muuten kortti havaitsee ainoastaan ne paketit, jotka on nimenomaan osoitettu kyseiselle kortille. Monitorointitilassa kortti havaitsee kaikki paketit, joita ilmassa kulkee.

MAC-osoitetta hyödynnetään käyttämällä niin sanottua pakettien haistelijaa (packet sniffer), joka tässä tapauksessa on airodump-ng, joka löytyy BackTrack 5 -ohjelmasta. Pakettien haistelijoilla voidaan puuttua tietoverkon liikenteeseen tai sitä voidaan tarkastella huomaamatta. Komento on muotoa airodump-ng --bssid 00:di:ce:fa:00 --channel 6 --write lihapulla mon0, missä:

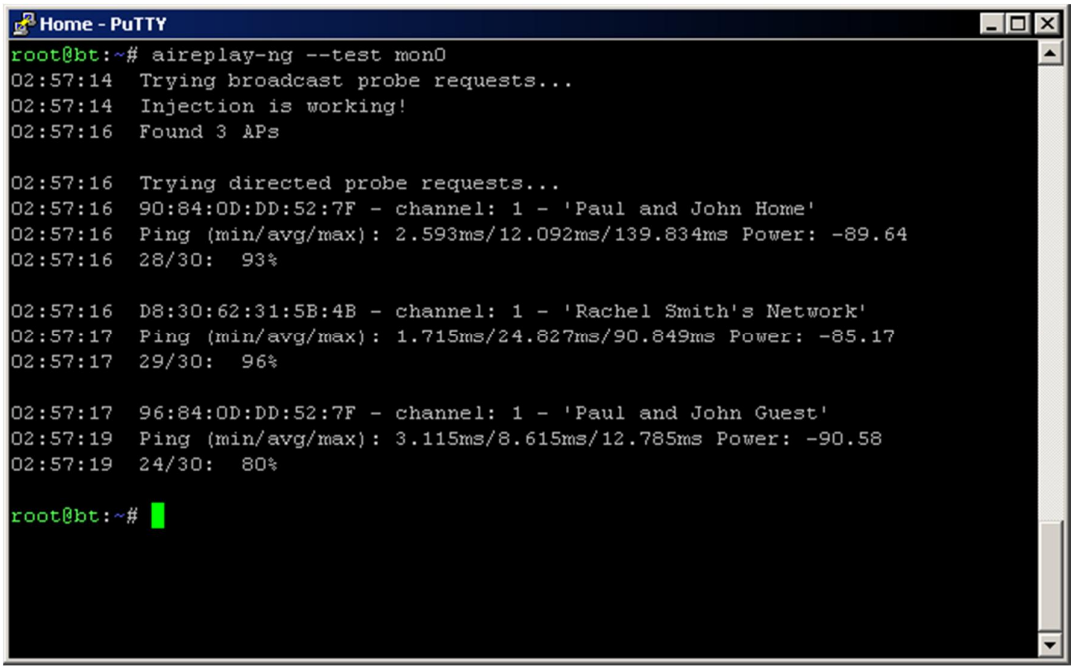
- --bssid 00:di:cd:fa:00 on yheyslaitteen MAC-osoite, johon halutaan yhteys muodostaa
- --channel 6 on kanava, jolla yhteyslaite toimii
- --write lihapulla kirjoittaa tiedoston nimeltä lihapulla, johon tulee tiedot esimerkiksi kättelytapahtumasta
- mon0 asettaa monitoroinnin päälle.

Kuva 10. BackTrack 5 R3:n pääsivu

Tämän jälkeen aletaan lähettää paketteja juuri luotuun lihapullatiedostoon. Aluksi tehdään niin sanottu de-authentication-hyökkäys, jolla voi esimerkiksi saada selville piilotetun SSID:n. Hyökkäys on käytännössä pakettien injektoimista pääkoneelle niin, että se saadaan katkaisemaan yhteys ja muodostamaan yhteyden uudelleen, jotta saadaan poimittua jaettu avain, jota käytetään kättelytapahtumassa, kun pääkone ottaa yhteyden langattomaan yhteyspisteeseen käyttämällä WPA:ta. Injektointi tapahtuu käyttämällä aireplay-ng:tä ja sen komento on muotoa aireplay-ng -0 3 -a 00:di:ce:fa:00 -c 00:14:aa:bb:55 mon0, missä:

- -0 määrittelee, että käytetään injektointipaketteja
- 3 kertoo lähetettävien pakettien määrän
- -a 00:di:ce:fa:00 kertoo langattoman yhteyspisteen MAC-osoitteen, johon paketit lähetetään
- -c 00:14:aa:bb:55 kertoo lähettäjän koneen MAC-osoitteen

- mon0 asettaa monitoroinnin päälle.



Kuva 11. Aireplay-ng pääsivu

Tämän jälkeen paketit lähtevät matkaan ja pääkoneen olisi pitänyt muodostaa yhteys uudelleen yhteyspisteeseen. Asia voidaan varmistaa käynnistämällä WireShark, jolla avataan luotu tiedosto, joka tässä tapauksessa on nimeltään lihapulla.cap. Tiedostosta löytyy protokolla sarake ja siellä pitäisi nyt näkyä EAPOL-tyyppinen tapahtuma, josta voidaan todeta, että yhteys on syntynyt uudelleen.

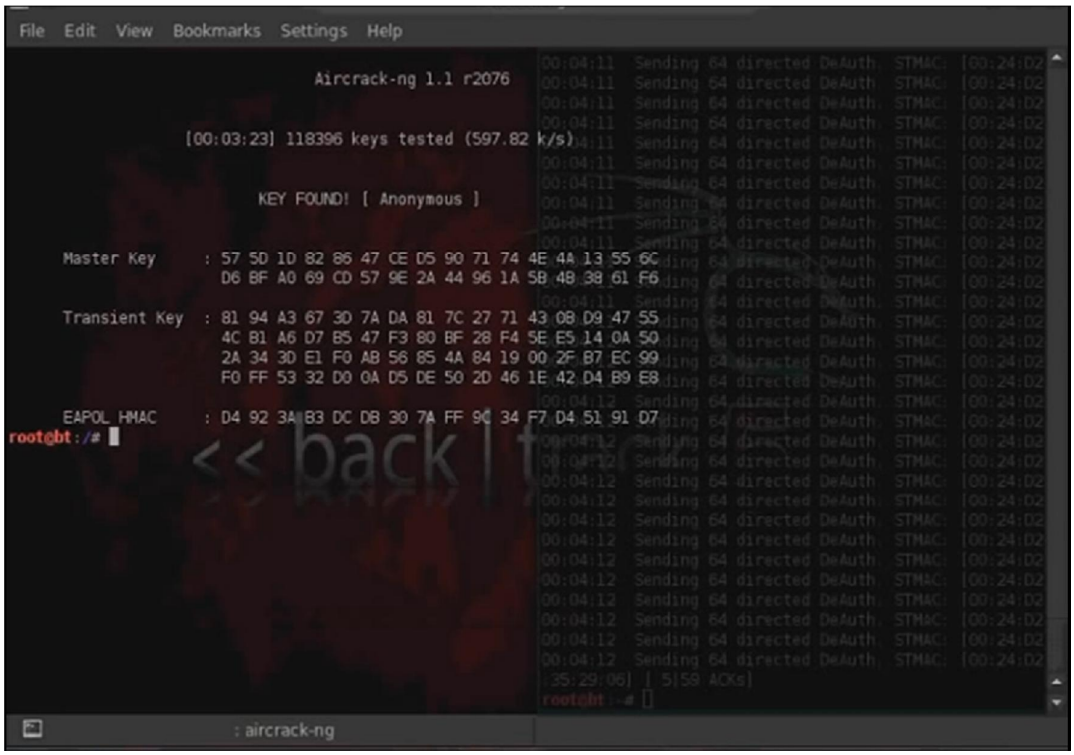
Nyt, kun yhteys on muodostettu ja se tiedetään, voidaan alkaa suorittamaan sanakirja-hyökkäystä eli niin sanottua brute force attack:ia aircrack-ng:llä, jossa ladataan aircrack-ng:lle mahdollisimman kattava salasana sanakirja, jota hyödynnetään hyökkäyksessä. Hyökkäys tapahtuu komennolla aircrack-ng lihapulla.cap -w /polku/polku1/salasanakirja.lst, missä:

- lihapulla.cap on tiedosto, johon kerättiin tiedot hyökkäyksen kohteesta
- -w /juuri/juuri1/salasanakirja.lst kertoo, että käytetään sanalistaa, joka löytyy spesifioidun polun päästä ja on nimeltään salasanakirja.lst.

Seuraavaksi ei tarvitse kuin odotella, että ohjelma käy salasanalistaa läpi ja vertaa niitä kohteena olevaan salasanaan. Koneen resursseista riippuen aikaa voi mennä hyvinkin pitkään, jos lista on erittäin pitkä eikä salasana selviä heti alussa.

Kun salasana vihdoin selviää, tulee se selkokielisenä näytölle. Samalla tulee hieman statistiikkaa siitä, kuinka monta avainta käytiin läpi ja kuinka monta avainta käytiin läpi sekunnissa ja kuinka kauan meni kokonaisuudessaan aikaa avaimen selvittämisessä.

Seuraavaksi testiä kannattaa toistaa siten, että etsii internetistä erilaisia salasanalistoja, joita yleensä hakkerit käyttävät apunaan murtautuessaan tietoverkkoihin, ja muuttaa oman reitittimen tietoturva-asetuksista salasanaksi joku sellainen, jonka itse luulee olevan turvallinen. Testiä toistetaan niin kauan, että keksii sellaisen salansanan, jota ei pysty ainakaan brute force attack -hyökkäyksellä löytämään. Samoin kannattaa kokeilla muitakin tietoturvaan liittyviä asetuksia reitittimeltä ja kokeilla mitä vaikutuksia on, jos SSID:tä ei näytetä ja sen jälkeen, jos se näytetään.



Kuva 12. Salasana anonymous on selvinnyt käyttämällä sanakirjaa

Tämä testi osoittaa, että periaatteessa langattoman verkon voi kuka tahansa peruskäyttäjäkin yrittää murtaa ja luultavasti siinä onnistuukin, jos vain riittää intoa ja viitseliäisyyttä. Sen takia kannattaakin olla jatkuvasti tarkkana ja yrittää testata näillä apuvälineillä oman verkon salasanan kestävyyttä ja turvallisuutta. Sellaista sanakirjaa ei varmasti ole olemassa, jossa olisi kaikki mahdolliset merkkijonojen variaatiot, joten pelkästään erikoismerkkien sisällyttäminen vähintään kolmetoista merkkiä pitkiin salasanoihin auttaa parantamaan oman verkon tietoturvaa huomattavasti.

6 Yhteenveto

Tietotekniikkaa ovat aina vaivanneet tietoturvauhat, eikä se asia todennäköisesti tule ikinä muuttumaan. Varsinkin langattomissa tietoverkoissa liikenteen kaappaaminen onnistuu melko pienellä vaivalla, jos vain on perehtynyt asiaan. Valitettavasti asiaan perehtyneitä henkilöitä riittää ja heidän tarkoitusperänsä eivät aina välttämättä ole hyvät, vaan he haluavat hyötyä käyttäjien langattomien verkkojen haavoittuvuuksilla joko rahallisesti tai saadakseen mainetta tai pilatakseen esimerkiksi jonkun yrityksen maineen.

Tässä työssä yritettiin hieman avata sitä, kuinka tavallinen käyttäjä voisi yrittää testata oman langattoman tietoverkkonsa turvallisuutta käyttämällä markkinoilla olevia ilmaisia ohjelmia. Ohjelmat ovat myös hakkereiden saatavilla, joten hekin niitä käyttävät, mutta heidän tarkoituksenaan on yrittää murtautua muihin kuin omiin verkkoihin. Sen takia mielestäni näiden ohjelmien käyttö oman langattoman yhteyden tietoturvan kokeiluun onkin järkevää. Ohjelmien tarkoituksena on lähinnä kaksi asiaa, haistella ja etsiä verkkoja, sekä kertoa niistä tietoa. Esimerkiksi Vistumbler pystyy kertomaan, onko löydettyjen yhteyspisteiden seassa jonkin sellainen, johon pääsee joko ilman salasanaa tai se on suojattu heikommalla WEP-kryptauksella. Aircrack-ng-ohjelmalla pystyykin tekemään osaavissa käsissä jo paljon enemmän, esimerkiksi sillä voi yrittää injektoida liikenteeseen vääränlaista tietoa tai sillä voi kaapata liikenteestä pakettaja, joita voi käsitellä vaikka WireSharkissa. Ohjelmalla voi myös yrittää murtaa salasanoja käyttämällä brute force attack -metodia, jolloin heikot salasanat paljastuvat jossain vaiheessa.

Jos käyttäjä ei kuitenkaan halua tai osaa käyttää tässä työssä mainittuja ohjelmia, toki muitakin on saatavilla vaikka kuinka paljon. Siinä tapauksessa kannattaa ehdottomasti

muistaa muutamia nyrkkisääntöjä liittyen langattoman verkon tietoturvaan. Ensimmäiseksi, piilotetaan verkon nimi eli SSID. Sitä on turha näyttää kaikille verkkoja haisteleville ohjelmille. Toiseksi, ei käytetä WEP-salausta, vaan aina, kun on mahdollista, joko WPA- tai WPA2-salausta. Kolmanneksi salasanoista tehdään riittävän kompleksisia, vähintään kolmetoista merkkiä pitkiä mitään tarkoittamattomia sanoja, joissa on seassa isoja ja pieniä kirjaimia, erikoismerkkejä sekä numeroita. Salasanan kompleksisuudesta huolimatta, yritetään tehdä salasanasta sellainen, että sen muistaa helposti itse, koska ei ole mitään järkeä keksiä mahdottomia salasanoja ja kirjoittaa niitä paperille näytön kulmalle tai näppäimistön alle muistiin.

Esimerkkinä kompleksisesta helpohkosti muistettavasta salasanasta voisi olla vaikka sanasta kalliolouhinta johdettu sana, jota hieman muokkaamalla saa vaikeasti arvattavan ja murrettavan salasanan. Pelkkä kalliolouhinta löytyy luultavasti jostain hakkerin salasanalistasta, joita ajetaan esimerkiksi aircrack-ng-ohjelmalla ja on erittäin todennäköistä, että salasana tulee murretuksi. Entä, jos sanan muuttaakin vaikka muotoon kAlL10louH1ntA!. Sana on jo huomattavasti kompleksisempi, mutta silti periaatteessa helposti muistettava ja sisältää nyt isoja- ja pieniä kirjaimia, numeroita ja erikoismerkin. Tuskin löytyy kenenkään hakkerin salasanalistoista tai mistään sanakirjoja apuna käyttävistä brute force -työkaluista. Salasanassa on jo mittaakin sen verran, että pelkästään jollain salasanageneraattorilla, joka kokeilisi lennossa erilaisia merkkijonoja ilman, että niitä olisi jo valmiiksi keksitty. Kestäisi todella kauan, ennen kuin se muodostaisi tuollaisen merkkijonon.

Tavallinen käyttäjä pystyy kyllä huolehtimaan langattoman laitteensa tietoturvasta, jos vain viitsii perehtyä laitteen ominaisuuksiin ja tietoturvaan liittyviin seikkoihin, kuten salausprotokolliin, pääsylistoihin, salasanoihin, verkon nimen piilottamiseen ja niin edelleen. Tietysti se vaatii hieman vaivaa ja aikaa, mutta omasta mielestäni nykyisin tietoturvauhat ovat olennainen osa tietotekniikkaa ja pieni panostaminen kannattaa, että saa nukkua yönsä rauhassa. Aina on olemassa riski, että joku pääsee murtautumaan luvattomasti laitteisiin, vaikka olisi yrittänyt suojata järjestelmänsä niin huolellisesti, kuin vain kykenee, mutta tärkeintä on, ettei tee siitä liian helppoa hakkereille. Jos hakkerit joutuvat näkemään tavallista enemmän vaivaa, he luultavasti etsivät helpomman kohteen, kuin hyvin suojatun langattoman yhteyden, sillä tuskin jokainen heistä hakee niitä suurimpia haasteita ja sitä kautta sulkia hattuunsa. Jos he haluavat meriitte-

jä, niin silloin he kohdistavat katseensa suurten yritysten tietoverkkoihin, ei tavallisen kuluttajan yksittäiseen langattomaan verkkoon.

Lähteet

1 Rosenblatt, S. 2013. Wi-Fi routers: More security risks than ever. Verkkodokumentti. <http://news.cnet.com/8301-1009_3-57596851-83/wi-fi-routers-more-security-risks-than-ever/>. Luettu 4.8.2013.

2 About IEEE. 2013. Verkkodokumentti. IEEE. <http://www.ieee.org/about/index.html>. Luettu 25.8.2013.

3 McCann, S., Ashley, A. 2013. Official IEEE 802.11 working group timelines - 2013-07-24. Verkkodokumentti. <http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm>. Luettu 25.8.2013.

4 Vaughan-Nichols, Steven J. 2013. High-speed 802.11ac Wi-Fi finally taking off. Verkkodokumentti. <http://www.zdnet.com/high-speed-802-11ac-wi-fi-finally-taking-off-7000019162/>. Luettu 12.9.2013.

5 Mitchell, B. 2013. SSID - Service Set Identifier in Wireless Computer Networking. Verkkodokumentti. <http://compnetworking.about.com/cs/wireless/g/bldef_ssid.htm>. Luettu 3.9.2013.

6 Subramanian, M., Gonsalves, T. & Rani, N. 2010. Network Management Principles and Practice. 1. painos. Noida, Intia: Dorling Kidersley (India) Pvt. Ltd.

7 Mitchell, B. WPA - Wi-Fi Protected Access in Computer Networking. Verkkodokumentti. <http://compnetworking.about.com/cs/wirelesssecurity/g/bldef_wpa.htm>. Luettu 14.10.2013.

8 Janssen, C. 2013. What is a rogue access point? Verkkodokumentti. <http://www.techopedia.com/definition/4082/rogue-access-point-rogue-ap>. Luettu 3.9.2013.

9 Rouse, M. 2013. What is distributed denial-of-service attack (DDoS)?. Verkkodokumentti. < http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack>. Luettu 3.9.2013.

10 Rouse, M. 2007. What is man in the middle attack (fire brigade attack)? Verkkodokumentti. <http://searchsecurity.techtarget.com/definition/man-in-the-middle-attack>. Luettu 3.9.2013.

11 Vesala, T, Qentinel. 2010. Tietoturvatestaus. Verkkodokumentti. <http://users.jyu.fi/~samiayr/testaus2010/Tietoturvatestaus-2010-03-24.pdf>. Luettu 20.8.2013

12 Kaner, C., Bach, J., Pettichord, B. 2002. Lessons learned in software testing. New York. John Wiley & Sons, Inc.

13 Wireshark. About. Verkkodokumentti.< http://www.wireshark.org/about.html>. Luettu 15.10.2013.

14 Geier, E. Network World. 2012. How to hack your own Wi-Fi network. Verkkodokumentti. <http://www.networkworld.com/news/2012/042312-hack-wifi-network-258477.html>. Luettu 15.2.2012.

15 Truth, S. How to Test for Man-in-the-middle Vulnerabilities. 2012. Verkkodokumentti. <http://web.securityinnovation.com/appsec-weekly/blog/bid/63269/How-to-Test-for-Man-in-the-Middle-Vulnerabilities>. Luettu 15.10.2013.